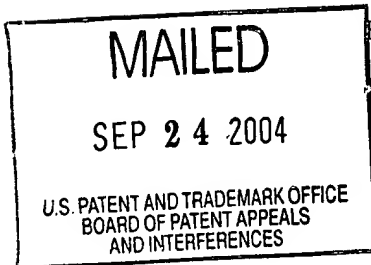


The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 31

UNITED STATES PATENT AND TRADEMARK OFFICE



BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MICHAEL A. EPSTEIN

Appeal No. 2003-1829
Application No. 08/994,878

ON BRIEF

Before THOMAS, GROSS, and BLANKENSHIP, *Administrative Patent Judges*.

GROSS, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 5 through 8, which are all of the claims pending in this application.

Appellant's invention relates to a method and system of utilizing private keys in a network environment wherein the private keys are not permanently stored on the user's equipment. Claim 5 is illustrative of the claimed invention, and it reads as follows:

Appeal No. 2003-1829
Application No. 08/994,878

5. A method for obtaining and using a private key at user equipment via a network, said method comprising:

transmitting from the user equipment an ID of a user;

receiving a private key of the user encrypted with a user identifying key associated with the user; and

decrypting the encrypted private key using a user identifying key determined from interaction with the user at the user equipment;

using the decrypted private key; and

destroying or avoiding making any non-volatile record of the private key at the location of the user.

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Asay et al. (Asay)	5,903,882	May 11, 1999 (filed Dec. 13, 1996)
Trostle	5,919,257	Jul. 06, 1999 (filed Aug. 08, 1997)

Bruce Schneier, Applied Cryptography 174 (2d ed., John Wiley & Sons, Inc. 1996) (Schneier)

Claims 5 and 7 stand rejected under 35 U.S.C. § 103 as being unpatentable over Trostle in view of Asay.

Claims 6 and 8 stand rejected under 35 U.S.C. § 103 as being unpatentable over Trostle in view of Asay and Schneier.

Reference is made to the Examiner's Answer (Paper No. 28, mailed April 7, 2003) for the examiner's complete reasoning in

Appeal No. 2003-1829
Application No. 08/994,878

support of the rejection, and to appellant's Brief (Paper No. 27, filed February 10, 2003) for appellant's arguments thereagainst.

OPINION

As a preliminary matter, we note that on page 4 of the Brief, appellant indicates that the claims are to stand or fall together. In accordance therewith, appellant has presented no separate arguments of patentability as to the dependent claims nor the additional reference of Schneier for claims 6 and 8. Therefore, we will treat the claims as a single group with claim 5 as representative. Appellant should note in accordance with 37 C.F.R. § 1.192(a) (which was in effect at the time of the Brief) arguments not included in the brief are considered waived. **See also, *In re Berger***, 61 USPQ2d 1523, 1529 (Fed. Cir. 2002) and ***Interactive Gift Express, Inc. v. Compuserve Inc.***, 256 F.3d 1323, 1344, 59 USPQ2d 1401, 1417 (Fed. Cir. 2001), in which the Federal Circuit held that issues not raised in the Brief are waived.

We have carefully considered the claims, the applied prior art references, and the respective positions articulated by appellant and the examiner. As a consequence of our review, we will affirm the obviousness rejections of claims 5 through 8.

Appellant argues (Brief, page 4) that Asay teaches storing an encrypted copy of the user's key at the location of the user, and, thus, Asay fails to teach the claim limitation of "destroying, or avoiding making, any non-volatile record of the private key at the location of the user." Appellant contends that Asay "specifically teaches **making, saving, and not destroying** at least one non-volatile record of the key." We disagree.

Asay discloses (column 7, lines 46-50) a subscriber (or user) "creating a standby application for certification of a new key pair, digitally signing the standby application with a private key **and then destroying the private key**" (emphasis ours). Similarly, Asay states (column 30, lines 55-57) that the private key is destroyed immediately after it is used to sign the standby application. Thus, Asay explicitly teaches destroying the private key at the user's terminal. Appellant argues (Brief, page 5) that the passage in column 30 follows a statement that the private key is stored in a safe place in the subscriber's system, and therefore teaches away from the "claimed destruction of any non-volatile record of the user's private key." However, the claim recites an alternative of "destroying **or** avoiding making" any non-volatile record of the private key. Although

Appeal No. 2003-1829
Application No. 08/994,878

Asay may initially store the private key on the user's system, Asay clearly teaches destroying it after it is used, thereby meeting the first claimed alternative.

Further, Asay teaches (column 27, lines 32-35) that "technological improvements may render the security of the key pair vulnerable to an attack facilitated by the availability of an accumulating body of ciphertext." Similarly, Asay discusses (column 28, lines 13-15) the risk of compromise of a private key. Therefore, Asay clearly teaches the need to destroy the private key so as to avoid rendering it vulnerable to an attack or to risk of compromise. Consequently, we find appellant's argument unpersuasive. Appellant has not argued the combinability of the references, nor presented any further arguments. Therefore, we will sustain the rejection of claims 5 through 8.

CONCLUSION

The decision of the examiner rejecting claims 5 through 8 under 35 U.S.C. § 103 is affirmed.

Appeal No. 2003-1829
Application No. 08/994,878

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

JAMES D. THOMAS
Administrative Patent Judge

Anita Pellman Gross
ANITA PELLMAN GROSS
Administrative Patent Judge

BOARD OF PATENT
APPEALS
AND
INTERFERENCES

Howard B. Blankenship
HOWARD B. BLANKENSHIP
Administrative Patent Judge

APG:clm

Appeal No. 2003-1829
Application No. 08/994,878

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510